Amendments to the Drawings:

The attached sheets of drawings include changes to FIGS. 1 and 4. FIG. 1 has been amended by changing "Kp ENCIPHERING UNIT" in item 160 to --Ks ENCIPHERING UNIT--. FIG. 4 has been amended by changing reference numeral "480" for the "SECOND DECODING UNIT" to --490-- to conform to the reference numeral 490 used throughout the specification for the second decoding unit.

Attachments: **Replacement Sheets** for FIGS. 1-5

Annotated Sheets Showing Changes to FIGS. 1 and 4

REMARKS

By the present amendment, the specification, FIGS. 1 and 4, and Claim 3 have been amended. Claims 1-10 remain pending in the application, with Claims 1, 3, 6, 7 and 10 being independent claims. The drawings and the specification are objected to because of informalities. Claims 1-10 are rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Akiyama (US 2003/0002680 A1).

Claim 3 has been amended to provide proper antecedent basis for a personal secret key ({Ks}Kh).

Replacement sheets for FIGS. 1-5 are submitted herewith, where FIG. 1 has been amended by changing "Kp ENCIPHERING UNIT" in item 160 to --Ks ENCIPHERING UNIT--, and FIG. 4 has been amended by changing reference numeral "480" for the "SECOND DECODING UNIT" to --490-- to conform to the reference numeral 490 used throughout the specification for the second decoding unit. The specification has also been amended to reflect consistent use of parentheses throughout the specification.

The amendments to FIGS. 1, 4, and the specification overcome the objections to the drawings and the specification. Applicant respectfully submits that the amendments to the drawings, the specification, and the claims are fully supported by the original disclosure, and introduce no new matter therewith.

Independent Claim 1 recites, in part, a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key

(Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M). Independent Claims 3, 6, 7 and 10 include similar recitations.

The Examiner relies on FIGS. 3, 14, paragraphs 107-108, 188 and 198 of Akiyama for satisfying all of the recitations of Claims 1-10.

Akiyama describes a broadcast reception device and a contract management device using a common master key in a conditional access system. Akiyama shows a contract management device in FIG. 3 that is provided at the broadcast station 200 shown in FIG. 1.

The present invention relates to a security deciphering apparatus and method in which the data of a cipher key used to encipher data is obtained by decoding an enciphered version of the cipher key by using hidden identification (ID) information given to a terminal requesting the data, so that an improvement in security can be achieved even for data transmitted over public networks. The present invention is characterized in that (1) a data service providing apparatus and each communication terminal share each hidden secret key (Kh) corresponding to intrinsic identification besides each (Kh) is received from the data service providing apparatus by each mobile communication terminal, and (2) it is determined whether data (M) is deciphered according to the sameness of the hidden secret key (Kh) in the data service providing apparatus and the communication terminal.

In contrast, compared with the present invention, Akiyama merely discloses how (1) a broadcast station 200 and each reception device 100 share an identical master key Km, and besides a terminal ID is deciphered by the master key Km previously stored in each reception device 100, and how (2) it is determined whether data (contents) are deciphered according to the sameness of the terminal ID in a reception device 100 and the broadcast station 200.

More specifically, referring to paragraph 110 of Akiyama, it is recited that the broadcast station 200 and each reception device 100 are provided with the identical master key Km, which is updated regularly by periods. Therefore, owing to using a same key in each reception

device 100 in Akiyama, any reception device 100 is capable of receiving any contents merely by handling a terminal ID.

In contrast, because the present invention teaches using different keys, which is intrinsic to each communication terminal, the security of Akiyama is weaker than that of the present invention.

More particularly, Akiyama fails to teach or reasonably suggest a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M), as recited in Claim 1. Akiyama also fails to teach or reasonably suggest similar recitations in independent Claims 3, 6, 7 and 10.

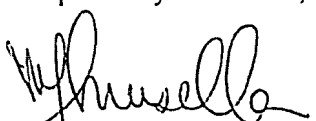
The Examiner has failed to establish a *prima facie* case of anticipation for at least these reasons.

Accordingly, Claims 1, 3, 6, 7 and 10 are allowable over Akiyama.

While not conceding the patentability of the dependent claims, *per se*, Claims 2, 4, 5, 8 and 9 are also allowable for at least the above reasons.

Accordingly, all of the claims pending in the Application, namely, Claims 1-10, are believed to be in condition for allowance. Early and favorable action is respectfully requested. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicant's attorney at the number given below.

Respectfully submitted,



Michael J. Musella
Reg. No. 39,310
Attorney for Applicant

THE FARRELL LAW FIRM
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
Tel: (516) 228-3565
Fax: (516) 228-8475

PJF/TCS/dr

Appl. No. 10/754,802
Art Unit 2135
Customer No. 66547
Confirmation No. 1597
Annotated Sheet Showing Changes

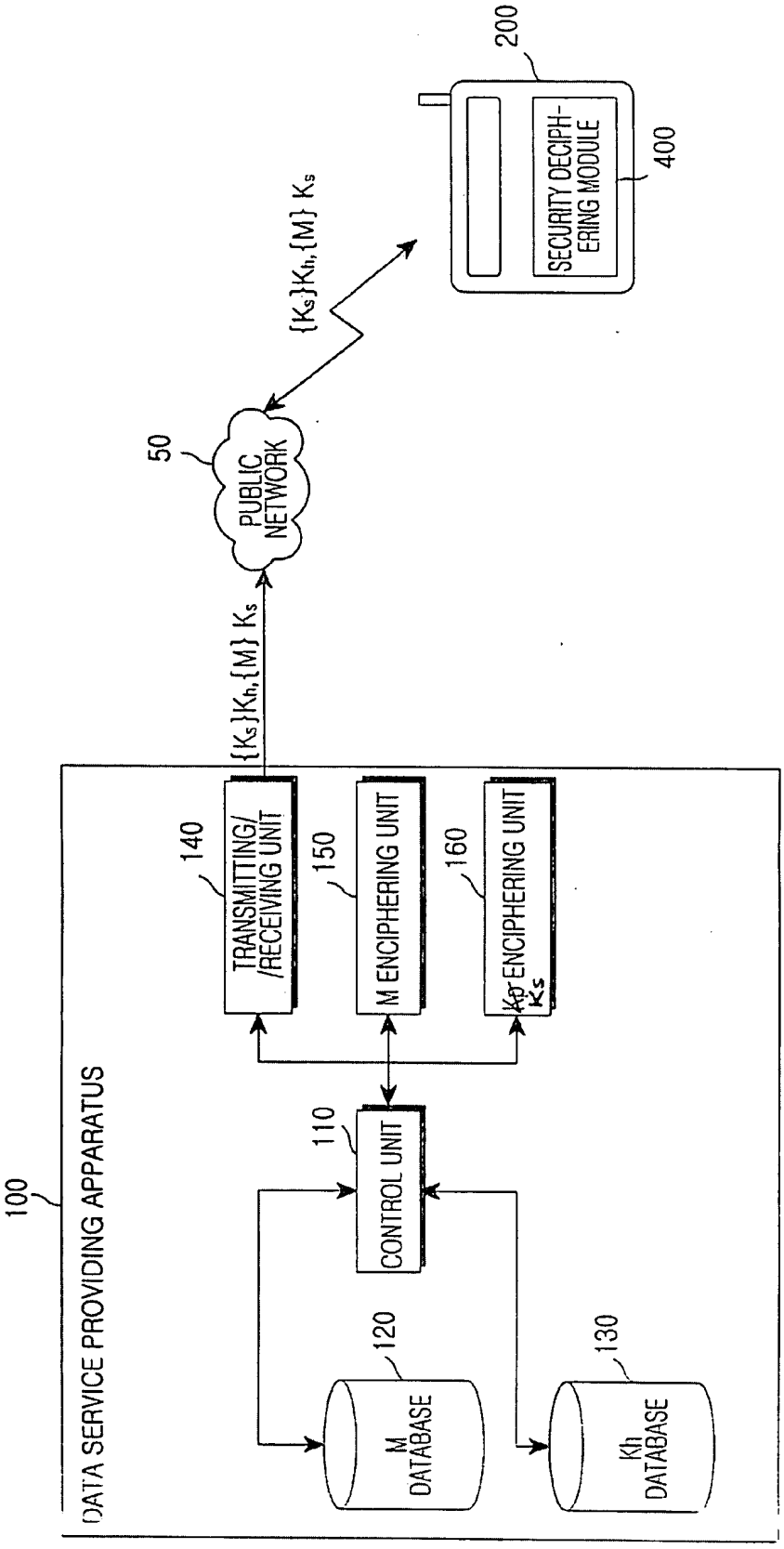


FIG. 1

Appl. No. 10/754,802
Art Unit 2135
Customer No. 66547
Confirmation No. 1597
Annotated Sheet Showing Changes

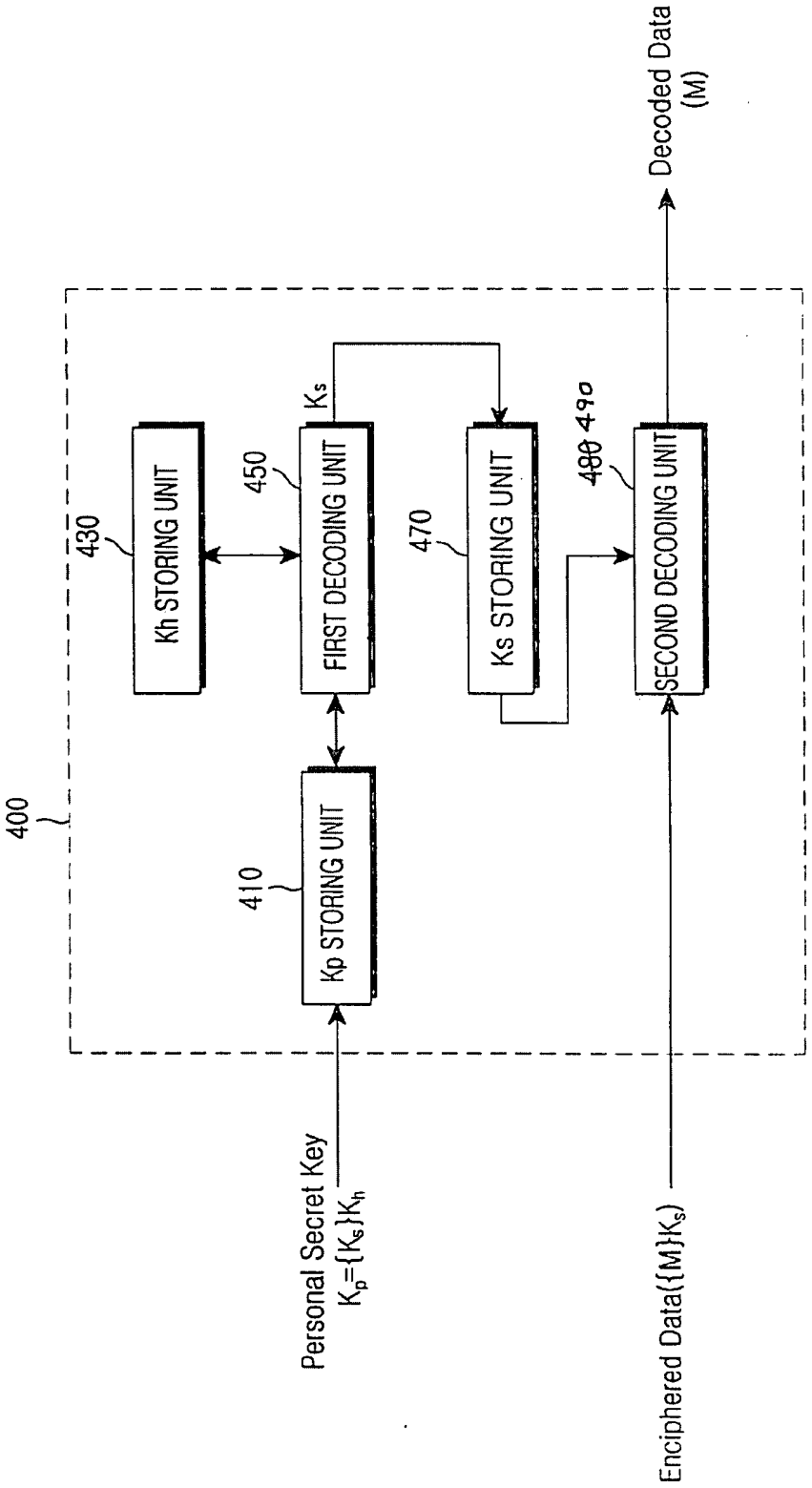


FIG. 4